SÄKERHETS- OCH INTEGRITETSSKYDDS-NÄMNDEN

YTTRANDE

Dnr
182-2023

2024-03-25

Justitiedepartementet
ju.remissvar@regeringskansliet.se
ju.da@regeringskansliet.se

# Hemlig dataavläsning – utvärdering och permanent lagstiftning (SOU 2023:78)

Ju2023/02690

Säkerhets- och integritetsskyddsnämnden (nämnden) har anmodats att yttra sig över innehållet i rubricerat betänkande.

Nämnden har granskat förslagen främst med utgångspunkt från sin uppgift att ur ett rättssäkerhets- och integritetsskyddsperspektiv utöva tillsyn över viss brottsbekämpande verksamhet.

## Sammanfattning

Nämnden, som anser att användningen av hemlig dataavläsning har inneburit en tydligt ökad risk för den personliga integriteten, avstyrker inte utredningens förslag att regleringen om hemlig dataavläsning ska göras permanent men är kritisk till att skyddet för den personliga integriteten anses väga så lätt.

Nämnden ställer sig delvis bakom utredningens förslag om hur regleringen om hemlig dataavläsning ska förtydligas. Nämnden har däremot invändningar mot förslagen om utökade möjligheter till hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brottet eller brotten. Behovet av att inhämta platsuppgifter och andra uppgifter som inte har kommunicerats från t.ex. en mobiltelefon som gärningsmannen har kontaktat framgår inte tydligt. Nämnden anser vidare att den föreslagna regleringen skulle utgöra en oacceptabel utvidgning av möjligheterna att använda hemliga tvångsmedel mot personer som är utomstående i förhållande till brottsutredningen och att förslaget i denna del inte lever upp till regeringsformens krav.

Nämnden avstyrker förslaget att villkor inte behöver anges i ett tillstånd till hemlig dataavläsning i vissa fall och framhåller bl.a. att det alltid finns ett behov av villkor som begränsar tillgången tidsmässigt om det, som utredningen föreslår, inte längre alltid behöver anges en gräns för tillståndets omfattning bakåt i tiden.

**Postadress**
Box 22523, 104 22 Stockholm

**Telefon**
08-617 98 00

**E-post**
sakint@sakint.se

**Organisationsnummer**
202100-5703

**Besöksadress**
Norr Mälarstrand 6, Stockholm

**Telefax**
08-617 98 88

**Webbplats**
www.sakint.se

**Bankgiro**
782-4329

Nämnden belyser en brist i en bestämmelse om förstöring av material från hemlig tvångsmedelsanvändning enligt rättegångsbalken och ifrågasätter om det är lämpligt att låta den bestämmelsen gälla även för hemlig dataavläsning. Vidare utvecklas skälen för att det bör vara den ansökande myndigheten i stället för rätten som ska underrätta nämnden om beslut om hemlig dataavläsning.

Avslutningsvis framhåller nämnden behovet av en samlad översyn av bestämmelserna om hemliga tvångsmedel.

## Bör bestämmelserna om hemlig dataavläsning göras permanenta? (kap. 6)

Nämnden har förståelse för att de brottsbekämpande myndigheterna har behov av effektiva verktyg för att kunna bekämpa allvarlig brottslighet men anser, som tidigare påtalats, att utvecklingen på lagstiftningsområdet är oroande utifrån de intressen nämnden har att bevaka. Det finns en uppenbar risk för att strävan efter att skyndsamt utreda och ge de brottsbekämpande myndigheterna utökade utredningsmöjligheter och nya verktyg, medför att behovet av analys och utvärdering av de sammantagna effekterna av redan lämnade och förväntade förslag får stå tillbaka. Ett exempel på detta är att det har gjorts flera ändringar i lagen (2020:62) om hemlig dataavläsning, trots att det rört sig om en tidsbegränsad lagstiftning som skulle komma att utvärderas. Vidare har det inte ingått i utredningens uppdrag att ens överväga om lagen ska förlängas i stället för permanentas. I sammanhanget kan det framhållas att såväl lagen (2007:978) om hemlig rumsavlyssning som lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) förlängdes innan regleringarna gjordes permanenta.

Utredningens samlade bedömning är att hemlig dataavläsning generellt sett inte innebär någon avsevärt ökad risk för den personliga integriteten. Nämnden vill mot den bakgrunden framhålla att nämnden utifrån sin erfarenhet, i likhet med vad lagstiftaren befarade vid införandet av lagen, tvärtom anser att användningen av hemlig dataavläsning har inneburit en tydligt ökad risk för den personliga integriteten.[1]

I betänkandet anförs vidare att hemlig dataavläsning har lett till förbättrade möjligheter att såväl förebygga, förhindra och upptäcka som utreda allvarlig

[1] Jfr prop. 2019/20:64 s. 92.

brottslighet mot enskilda och att tvångsmedlet i det avseende har inneburit ett förstärkt skydd för enskildas personliga integritet. Detta används även som ett argument för att det är proportionerligt att permanenta lagstiftningen. Nämnden invänder inte mot bedömningen att hemlig dataavläsning har medfört sådana förbättrade möjligheter som utredningen gör gällande, men anser att utredningen tillmäter argumentet för stor vikt. Det kan användas för att rättfärdiga införandet av vilka ingripande tvångsmedel som helst, så länge de har någon nytta. Till detta kommer den omständigheten att hemlig dataavläsning till övervägande del har använts för att utreda narkotikabrottslighet,[2] vilket inte kan sägas utgöra allvarlig brottslighet mot enskilda.

Nämnden vill mot den nu angivna bakgrunden inte avstyrka en permanentning av lagen men är kritisk till att skyddet för den personliga integriteten anses väga så lätt.

## Tillämpningsområdet för hemlig dataavläsning (kap. 7)

### Bör innebörden av hemlig dataavläsning förtydligas? (avsnitt 7.2)

Nämnden delar bedömningen att uttrycket ”inhämtas” i stället för ”läses av eller tas upp” i definitionen av hemlig dataavläsning medför en tydligare reglering som i större utsträckning återspeglar sättet som tvångsmedlet verkställs. Nämnden tillstyrker därför förslaget i denna del.

### Uppgiftstyper och differentiering (avsnitt 7.3)

Enligt utredningens förslag ska uppgiftstyperna i punkt 6 och 7 ersättas av en ny punkt 6 som avser uppgifter som är åtkomliga i ett avläsningsbart informationssystem men som inte avses i 2 § första stycket 1–5 lagen om hemlig dataavläsning (punkt 6-uppgifter).

Nämnden konstaterar att förslaget försämrar möjligheterna att genom uppgiftstyper differentiera åtgärden. I den hittillsvarande tillämpningen har dock tillstånd till hemlig dataavläsning avseende endast en av punkterna 6 eller 7 inte varit vanliga. Dessutom innebär förslaget att det finns möjlighet att genom villkor begränsa tillståndet till att avse t.ex. endast uppgifter om hur det avläsningsbara informationssystemet används, om det är ändamålsenligt i det enskilda fallet. Mot den bakgrunden anser nämnden att förslaget om en ny

[2] Jfr skr. 2023/24:47 s. 30–31.

punkt 6 i 2 § första stycket lagen om hemlig dataavläsning får anses godtagbart.

Utredningen föreslår vidare att ett tillstånd till hemlig dataavläsning ska omfatta uppgiftstyperna i den föreslagna bestämmelsen i 2 § första stycket 1–3 och 6 lagen om hemlig dataavläsning, om inget annat särskilt beslutas eller framgår av andra bestämmelser. Detta kan sägas vara en kodifiering av den praxis som nämnden har kunnat iaktta vid tillsynen av hur regleringen tillämpas.[3] Nämnden ser emellertid en risk för att förslaget kan medföra att det än mer sällan kommer att förekomma att åtgärden differentieras på det sätt som avsågs när lagen infördes. Det är därför positivt att det i författningskommentaren framhävs att den föreslagna huvudregeln inte förändrar den ordningen att åtgärden ska differentieras i det enskilda fallet.

## Nya möjligheter att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet (avsnitt 7.4.4)

### Utökade möjligheter till hemlig dataavläsning avseende punkt 2, 3 och 6-uppgifter i syfte att utreda vem som skäligen kan misstänkas för brott

Utredningen föreslår att det ska införas utökade möjligheter till hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brottet eller brotten. Om tillståndet gäller uppgiftstyperna i den föreslagna 2 § första stycket 2, 3 eller 6 lagen om hemlig dataavläsning, ska åtgärden få avse dels ett avläsningsbart informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten under den tid som tillståndet avser har använt eller kommer att använda, dels ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Möjligheten att använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning för motsvarande uppgiftstyp i syfte att utreda vem som skäligen kan misstänkas infördes så sent som den 1 oktober 2023. I nämndens remissyttrande över det betänkande som låg till grund för lagändringen framhölls att förslaget innebär en stor förändring och att tvångsmedelsanvändningen blir mindre förutsebar och riskerar att i större utsträckning riktas mot personer som visar sig vara varken misstänkta eller på annat sätt in-

[3] Se nämndens uttalande den 15 november 2023 ”Otillåten tilläggsinformation och differentiering vid användning av hemlig dataavläsning” (dnr 161-2022).

tressanta för brottsutredningen. Nämnden underströk därför vikten av att lagrade uppgifter och användningsuppgifter enligt punkterna 6 och 7 i 2 § första stycket lagen om hemlig dataavläsning skulle undantas.[4]

Företrädare för Polismyndigheten har för den nu aktuella utredningen framhållit att inhämtning av punkt 6-uppgifter skulle möjliggöra en analys där digitala spår från olika håll kombineras och utreds parallellt i syfte att upptäcka eventuella samband, vilket många gånger är en förutsättning för att kunna identifiera personerna bakom brottsligheten. Med beaktande av detta resonemang, som utvecklas vidare och exemplifieras i betänkandet, anser nämnden att utredningens förslag framstår som acceptabelt såvitt avser ett avläsningsbart informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda. Nämnden ställer sig däremot frågande till att åtgärden såvitt avser platsuppgifter och, i synnerhet, punkt 6-uppgifter föreslås kunna omfatta ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Nämnden anser att behovet inte har belysts på ett tillräckligt tydligt sätt i denna del. Utöver kommunikationsavlyssningsuppgifter, som får inhämtas enligt den nuvarande regleringen, har nämnden förståelse för behovet av att få tillgång till kommunikationsövervakningsuppgifter som är åtkomliga i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta. Det är däremot oklart varför platsuppgifter och punkt 6-uppgifter behöver inhämtas från ett sådant informationssystem. Den ovan nämnda analysen av digitala spår avser, såvitt betänkandet får förstås, enbart uppgifter som är åtkomliga i avläsningsbara informationssystem som används av gärningsmän eller medverkande till brottsligheten.

Vidare innebär förslaget att det blir möjligt att inhämta precisa uppgifter om geografisk positionering avseende en person som den misstänkte gärningsmannen eller någon annan som har medverkat till brottet eller brotten enbart har kontakt med. Det blir också möjligt att inhämta t.ex. privata anteckningar eller bild- och filmfiler som inte har delats med någon, trots att det inte finns

[4] Nämndens yttrande den 21 september 2022 över betänkandet Utökade möjligheter att använda hemliga tvångsmedel (SOU 2022:19) (dnr 87-2022).

särskild anledning att anta det avläsningsbara informationssystem i vilket uppgifterna är åtkomliga har använts eller kommer att användas av gärningsmannen eller någon annan som har medverkat till brottsligheten. Även om platsuppgifter och punkt 6-uppgifter som är åtkomliga i ett sådant informationssystem teoretiskt skulle vara av värde för identifieringen av en misstänkt gärningsman i ett enskilt fall, anser nämnden att förslaget utgör en oacceptabel utvidgning av möjligheterna att använda hemliga tvångsmedel mot personer som varken är misstänkta eller bedöms vara gärningsmän eller medverkande till brottsligheten. Enligt nämnden lever förslaget inte upp till de krav som regeringsformen ställer på lagstiftning som begränsar skyddet mot betydande intrång i den personliga integriteten.

Mot den bakgrunden avstyrker nämnden förslaget i den del det avser platsuppgifter och punkt 6-uppgifter som är åtkomliga i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

**Hemlig dataavläsning avseende kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott**

Utredningen föreslår att ett tillstånd till hemlig dataavläsning avseende kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas ska få verkställas på en plats som är någons stadigvarande bostad, om det finns synnerliga skäl.

Nämnden delar utredningens uppfattning att bestämmelsen, om den införs, bör utformas på ett sätt som innebär att tillämpningsområdet för åtgärden blir mycket begränsat. Förslaget innebär att det ska krävas synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser. Utredningen anser att detta, tillsammans med den grundläggande förutsättningen att åtgärden ska vara av synnerlig vikt för utredningen, innebär att det är proportionerligt att införa undantaget. Nämnden delar inte den bedömningen. Synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystemet är ett krav som tar sikte på kopplingen mellan personen och informationssystemet och utgör i praktiken inte ett begränsande kvalifikationskrav. Det är inte ovanligt att en elektronisk kommunikationsutrustning används av endast en person och det ligger i sakens natur att den person som använder t.ex. en mobiltelefon befinner sig i närheten av den. Det innebär att kravet som huvudregel kommer

att vara uppfyllt när övriga krav är uppfyllda och det avläsningsbara informationssystemet används i någons stadigvarande bostad. Detta står i strid med utredningens avsikt att ställa upp höga, begränsande krav för tillämpningen. Enligt nämndens mening bör undantaget endast införas om kraven för tillämpningen utformas på ett mer inskränkande sätt.

## Kontrollmekanismerna och andra rättssäkerhetsgarantier (kap. 8)

### Förtydliganden om tillståndets varaktighet (avsnitt 8.4.4)

Enligt nuvarande reglering ska det i ett tillstånd till hemlig dataavläsning anges vilken tid tillståndet avser. Utredningen föreslår att det i stället ska anges under vilken tid som verkställighet får äga rum. Tiden för verkställighet får enligt förslaget inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Förslaget innebär att inhämtning av lagrad information däremot inte behöver begränsas bakåt i tiden. Sådana begränsningar kan i stället anges genom villkor i tillståndet.

Nämnden ser positivt på att den föreslagna regleringen gör det klart att verkställighetsförsök får göras under som längst en månad från beslutet. Enligt nämnden finns det dock inte skäl att helt frångå kravet på att åtgärden ska begränsas även bakåt i tiden. Kravet bidrar nämligen till att tillstånd inte ges en mer omfattande utformning än vad som är nödvändigt i det enskilda fallet. Med beaktande av de tekniska svårigheterna att under inhämtningen tidsbestämma lagrad information har nämnden förståelse för utredningens förslag. Det utgör dock en betydande förändring av regleringen och ställer stora krav på åklagaren och ytterst rätten att regelmässigt ställa upp villkor som kan tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Med hänsyn till den hittillsvarande användningen av villkor och förslaget om att villkor inte ska anges om det bedöms vara obehövligt (se nästa avsnitt), ser nämnden en uppenbar risk för att tidsmässigt begränsande villkor sällan kommer att användas och att åtgärden därmed tillåts bli långt mer omfattande än i dag. Enligt nämnden kan förslaget därför enbart godtas om det införs ett krav på att ett beslut om tillstånd avseende andra uppgiftstyper än kamera-

övervaknings- och rumsavlyssningsuppgifter alltid ska förenas med villkor som tar sikte på tidsmässiga avgränsningar.[5]

Som utredningen framhåller bör villkor, om det är möjligt och ändamålsenligt, avse inhämtningen och i annat fall bearbetningen av det inhämtade materialet. Eftersom det inte finns skäl att frångå den nuvarande ordningen mer än nödvändigt anser nämnden att detta är särskilt viktigt i fråga om villkor som begränsar åtgärden bakåt i tiden.

### Förtydligande om villkor för tillståndet (avsnitt 8.4.5)

Nämnden har tidigare konstaterat att regleringen om villkor vid användningen av hemlig dataavläsning inte har fungerat i enlighet med lagstiftarens avsikt.[6] Det har ofta förekommit tillstånd som antingen saknat villkor eller haft standardiserade villkor utan någon egentlig innebörd. Mot den bakgrunden är nämnden positiv till förslaget att åklagaren, eller i förekommande fall Säkerhetspolisen, i samband med en ansökan om hemlig dataavläsning ska föreslå villkor.

Förslaget att villkor inte ska anges om det framstår som obehövligt inger dock betänkligheter. Nämnden ser en tydlig risk för att villkor i en stor andel fall inte kommer att ställas upp med hänvisning till att det är obehövligt, trots att det verkliga skälet till att villkor inte anges är att det krävs en inte obetydlig arbetsinsats för att formulera villkor som innebär en ändamålsenlig och utifrån den enskildes personliga integritet lämplig begränsning i det enskilda fallet. Utredningen har visserligen på ett förtjänstfullt sätt redogjort för olika exempel på villkor, men nämnden anser likväl att denna risk är överhängande så länge det finns ett undantag från huvudregeln att villkor ska anges. Vidare anser nämnden, av de skäl som har anförts i föregående avsnitt, att det alltid finns ett behov av tidsmässigt begränsande villkor om förslaget om tillståndets varaktighet införs. Nämnden avstyrker därför förslaget att villkor inte behöver anges i ett tillstånd till hemlig dataavläsning om det framstår som obehövligt.

I sammanhanget vill nämnden även framhålla vikten av att villkor utformas på ett sätt som medför att det är rätten som tar ställning till hur inhämtningen eller granskningen ska begränsas. Standardiserade villkor i linje med ”endast uppgifter som är av betydelse för utredningen av brottet får granskas” innebär

[5] Inhämtning av kameraövervaknings- och rumsavlyssningsuppgifter avser alltid realtidsuppgifter, varför någon begränsning bakåt i tiden inte är aktuell för dessa uppgiftstyper.
[6] Nämndens uttalande den 20 juni 2023 ”Användningen av villkor vid ansökan om hemlig dataavläsning" (dnr 80-2022).

att det är åklagaren eller den verkställande myndigheten som bedömer vad som är relevant och därmed tillåtet att granska. Användning av sådana villkor urholkar tillståndsprövningen och de är enligt nämndens mening inte godtagbara. Enligt nämnden är de exempel på villkor som nämns i betänkandet tillfredsställande i detta avseende. Med hänsyn till den användning av villkor som nämnden har kunnat iaktta hittills finns det dock anledning att i författningskommentaren förtydliga att standardiserade villkor som i praktiken låter åklagaren eller den verkställande myndigheten fritt bestämma vad som ska inhämtas eller under bearbetningen sorteras bort aldrig får förekomma.

### Särskilt om kravet att ange vilket avläsningsbart informationssystem tillståndet avser (avsnitt 8.4.6)

Nämnden delar utredningens bedömning att kravet på att det i tillståndet ska anges vilket avläsningsbart informationssystem som tillståndet avser är tydligt och uppfyller de rättssäkerhetskrav som ställs på lagstiftningen. Till skillnad från utredningen anser nämnden dock inte att formuleringen ”det eller de Facebook-konton som används från den aktuella utrustningen, om det inte är uppenbart att de tillhör en annan person än den misstänkte”, utgör ett exempel på en tillräckligt rättssäker och specifik avgränsning. En sådan specificering innebär att en del av den tillståndsprövning som ska göras av rätten – nämligen bedömningen av om det finns tillräcklig koppling mellan den berörda personen och det avläsningsbara informationssystemet – förskjuts till den verkställande myndigheten. Enligt nämnden är det inte godtagbart med hänsyn till den rättssäkerhetsgaranti som tillståndsprövningen ska utgöra.[7]

### Användning av överskottsinformation (avsnitt 8.5.3) och granskning, bevarande och förstöring (avsnitt 8.5.4)

Utredningen föreslår att reglerna om användning av överskottsinformation och om granskning, bevarande och förstöring av upptagningar och uppteckningar från hemlig dataavläsning under en förundersökning ska ändras i enlighet med de regler som trädde i kraft i rättegångsbalken den 1 oktober 2023.

Något förenklat innebar den tidigare regleringen i 27 kap. 24 § rättegångsbalken att upptagningar och uppteckningar skulle bevaras till dess att ärendet avslutats och att de därefter skulle förstöras. Förstöringsskyldigheten gällde dock inte sådana uppgifter från upptagningar och uppteckningar som fick an-

[7] Se vidare nämndens uttalande den 29 mars 2023 ”Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Linköping” (dnr 43-2022).

vändas som s.k. överskottsinformation. Det berodde på att regeln om förstöring avsåg upptagningar och uppteckningar – inklusive sådana som har överlämnats till t.ex. en annan förundersökning – men inte uppgifter från sådant material.[8]

I den nya regleringen i 27 kap. 24 § rättegångsbalken anges att uppgifter – inte, som tidigare, upptagningar och uppteckningar – ska förstöras när de inte längre ska bevaras. Även om avsikten med lagändringen som trädde i kraft den 1 oktober 2023 inte var att åstadkomma någon förändring i detta avseende innebär bestämmelsens ordalydelse enligt nämnden att förstöringsskyldigheten omfattar samtliga uppgifter, dvs. även sådana som t.ex. har överlämnats till Polismyndighetens underrättelseverksamhet och som tidigare undantogs från förstöringsskyldigheten.[9]

Eftersom avsikten med utredningens förslag förefaller vara att uppgifter som utgör överskottsinformation ska kunna bevaras även efter ett beslut om förstöring kan det ifrågasättas om det är lämpligt att – utan föregående justering i 27 kap. 24 § – låta rättegångsbalkens nuvarande bestämmelser om förstöring gälla även för hemlig dataavläsning.[10]

### Särskilt om inhämtning av uppgifter i strid mot lagen om hemlig dataavläsning (avsnitt 8.5.6)

Utredningen föreslår att upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor i ett tillstånd till hemlig dataavläsning ska förstöras i de delar de innehåller sådana uppgifter och att det ska göras så snart det står klart att sådana uppgifter har inhämtats eller granskats.

Nämnden anser att det är positivt att förslaget bidrar till att det inte bevaras fler inhämtade uppgifter än vad som är nödvändigt. Enligt nämnden finns det

[8] Jfr SOU 2018:61 s. 206–208.

[9] Förslaget från Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel innebar att lagtextens distinktion mellan upptagningar och uppteckningar respektive uppgifter från sådant material fanns kvar, se SOU 2018:61 s. 26–27. I propositionen anger regeringen inte varför den frångick utredningens förslag om bestämmelsens utformning, se prop. 2022/23:126 s. 182–185 och 222.

[10] Med hänsyn till utformningen av motsvarande bestämmelser i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, preventivlagen och lagen (2022:700) om särskild kontroll av vissa utlänningar gör sig den beskrivna problematiken inte gällande när det kommer till hemlig dataavläsning utanför en förundersökning.

dock anledning att ytterligare analysera hur den föreslagna regleringen förhåller sig till Europadomstolens praxis.

Utredningen anför, till stöd för sin slutsats att förslaget inte står i strid med Europakonventionen, bl.a. att det innebär att den berörde själv bör ha tillgång till de uppgifter som kommer att förstöras. Den föreslagna regeln om förstöring av uppgifter som inte får inhämtas eller granskas enligt villkor tar emellertid sikte på inte bara uppgifter som den berörde har tillgång till, utan även uppgifter som av olika skäl inte är åtkomliga för den berörde i efterhand. Det kan t.ex. handla om meddelanden som inhämtas i realtid av den verkställande myndigheten men som till följd av hur meddelandetjänsten fungerar inte lagras på den berördes avläsningsbara informationssystem. Vidare kan det handla om att den berörde själv raderar uppgifter som sedan tidigare inhämtats av den verkställande myndigheten. Den berörde kommer alltså inte alltid att ha tillgång till inhämtade uppgifter som ska förstöras enligt villkor. Det förhållandet behöver analyseras närmare i det fortsatta lagstiftningsarbetet.

### Tillsyn och annan efterhandskontroll (avsnitt 8.7)

Utredningen föreslår att skyldigheten att underrätta nämnden om beslut om hemlig dataavläsning även i framtiden ska gälla för domstolarna. Enligt nämnden bör det i stället vara den ansökande myndigheten, dvs. åklagaren eller i förekommande fall Säkerhetspolisen, som ska underrätta nämnden.[11]

Nämnden kan konstatera att domstolarnas underrättelser i ett inte obetydligt antal fall är ofullständiga eller felaktiga, vilket leder till att nämndens kansli behöver inhämta kompletteringar eller rättelser. Det är inte osannolikt att det även förekommer felaktiga uppgifter i underrättelserna som inte framgår på ett sådant sätt att det uppstår anledning att kontrollera uppgifterna. Vidare kan det inte uteslutas att en domstol i något fall förbiser att över huvud taget underrätta nämnden om beslut om hemlig dataavläsning.

Eftersom nämndens tillsyn inte omfattar domstolarnas verksamhet kan nämnden inte granska efterlevnaden av underrättelseskyldigheten. Det är beklagligt med hänsyn till att skyldigheten, som utredningen framhåller, utgör ett viktigt led i den efterhandskontroll som är nödvändig för att säkerställa en rättssäker

[11] Sedan den 1 oktober 2023 gäller även att rätten skyndsamt ska underrätta nämnden när den har beslutat i frågor om tillstånd till tvångsmedel enligt 1 a § preventivlagen. Underrättelseskyldigheten enligt den lagen omfattas inte av det nu aktuella lagstiftningsärendet. Nämndens synpunkter på underrättelseskyldigheten enligt lagen om hemlig dataavläsning gör sig emellertid även gällande i fråga om motsvarande skyldighet enligt preventivlagen.

användning av hemlig dataavläsning. Om underrättelseskyldigheten i stället läggs på den ansökande myndigheten har nämnden möjlighet att rikta kritik mot handläggningen i fall där nämnden tar emot felaktiga underrättelser eller där det på något sätt uppmärksammas att en underrättelse har förbiseetts. En sådan ordning skapar bättre förutsättningar för att underrättelseskyldigheten ska kunna utgöra ett reellt led i efterhandskontrollen.

I sammanhanget kan det noteras att skyldigheten att underrätta nämnden om beslut enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ligger på den ansökande myndigheten, dvs. Polismyndigheten, Tullverket eller Säkerhetspolisen. En ordning där underrättelseskyldigheten gäller för myndigheter som står under nämndens tillsyn har således ansetts lämplig i en annan reglering om hemliga tvångsmedel.

## Lagstiftningens struktur och placering (kap. 9)

Utredningen bedömer att det bör göras en samlad översyn av området för tvångsmedel. Nämnden delar den bedömningen såvitt avser hemliga tvångsmedel. Behovet av en samlad översyn av bestämmelserna om hemliga tvångsmedel är också något som Lagrådet nyligen har framhållit.[12] Nämnden förutsätter att en sådan översyn är en prioriterad fråga för regeringen.

---

Detta yttrande har beslutats av Säkerhets- och integritetsskyddsnämnden. I beslutet har Gunnel Lindberg (ordförande), Anti Avsan, Charlotta Bjälkebring Carlsson, Matheus Enholm, Stephen Jerand, Jon Karlfeldt, Helene Odenjung och Per Schöldberg deltagit.

Föredragande har varit Viktor Wallén.

Gunnel Lindberg

[12] Lagrådets yttrande den 11 januari 2024 över lagrådsremissen Bättre möjligheter att verkställa frihetsberövanden.